SLAUGHTER AND MAY/

CLIENT BRIEFING

NOVEMBER 2021

DIVERGENCE, CONVERGENCE AND CHALLENGES: TRENDS IN GDPR ENFORCEMENT ACROSS EUROPE AND THE UK

A version of this article first appeared in the Privacy Law s & Business UK Report, Issue 118 (November 2021)

The introduction of the General Data Protection Regulation (EU) 2016/679 (the "**GDPR**") in May 2018 was a dramatic step forward in empowering data protection authorities ("**DPAs**") across the EU to tame the 'wild west' of the new digital economy and safeguard data rights. Post-Brexit, the UK has (so far) maintained this data protection enforcement framework through the retention of the GDPR in UK domestic law (as the "**UK GDPR**").

The GDPR's immediate impact was perhaps felt most in compliance programmes but, over three years in, clearer enforcement (and litigation) trends are emerging. This article considers three such trends:

a. First, despite the GDPR's common framework, there are signs of divergence (as well as convergence) in enforcement strategies and priorities both among EU DPAs as well as between the EU and the UK.

b. Second, the challenges (and delays) to resolving DPA investigations and potential enforcement remain significant, both for regulators and regulated.

c. Third, the role of the courts is becoming increasingly important, whether in deciding appeals against DPA decisions or providing an alternative source of redress for individual data subjects.

In each case, a key challenge for DPAs, courts and data controllers is prioritising those breaches, incidents or claims that present the greatest risk to data subjects' rights while allowing innovative business to flourish.

Divergence in GDPR enforcement activity and fines

The GDPR was expected to revolutionise enforcement by DPAs, in particular by:

a. requiring data controllers to 'self-report' breaches involving a risk to data subjects' rights to their relevant DPA (Article 33);

b. giving DPAs enhanced enforcement powers, providing for fines of up to 4% of an offender's global turnover or €20 million for the most serious violations (Article 83); and

c. introducing the Article 60 'one-stop shop' mechanism and pre-enforcement consultation process between EU DPAs (no longer including the UK's Information Commissioner's Office ("**ICO**")

However, there has been some divergence in the practical implications of these changes. For instance, there was initially considerable focus on data breaches and the potential consequential enforcement. In 2019 and 2020, EU DPAs received over 200,000 data breach notifications with the number of fines issued by EU DPAs doubling from 2018 to 2021.

In the UK, there was a significant focus on the headline BA and Marriott cases in 2019/2020. However, the ICO's 2020/2021 annual report recorded a c.20% reduction in data breach notifications against financial year 2019/2020 with only 21.6% of breaches notified resulting in investigation and only 0.1% leading to a fine.

From an EU perspective, the European Data Protection Board ("**EDPB**") published draft guidelines on data breaches and mandatory notifications in January 2021, drawn from the practical experience of EU DPAs. These worked through a number of scenarios, including 'advisable measures' controllers can implement to comply with their GDPR obligations and mitigate the risks of a data breach occurring (or leading to enforcement action). However, as the obligation to report remains relatively clear, the draft guidelines are unlikely to reduce EU DPAs' enforcement activity significantly.

As a general trend, EU DPAs have proven more willing than the ICO to use their enhanced powers and have issued record fines under the GDPR in 2021. In August 2021, Luxembourg's National Data Protection Commission ("**CNPD**") imposed a €746,000,000 fine on Amazon Europe Core S.à.r.l. ("**Amazon**") for non-compliance with general data processing principles - by far the largest GDPR fine issued to date.

Strikingly, the fine imposed on WhatsApp Ireland Limited ("**WhatsApp**") in September 2021, also for non-compliance with general data processing principles, was increased to

€225,000,000 after the EDPB directed Ireland's Data Protection Commission ("**DPC**") to increase the fine. The DPC had originally proposed fining WhatsApp between €30,000,000 and €50,000,000, resulting in challenges from eight other EU DPAs, and the DPC triggering the EU GDPR's dispute resolution process (Article 65). However uncertainty remains on the approach to fines; the EDPB directed that turnover may be considered for the calculation of the fine to ensure that it is "effective, proportionate and dissuasive" (Article 83). This corresponds with the ICO's inclusion of turnover as an appropriate starting point as part of its nine steps in determining the level of a fine under the UK GDPR[1]. However, this turnover-centred approach is at odds with the November 2020 decision of Germany's Bonn Regional Court, which held, in an appeal brought by 1&1 Telecom GmbH against a DPA fine, that turnover is not a decisive factor and should merely provide the overall framework for calculating a fine.

Despite the common framework of the GDPR, the ICO appears to have taken a less enforcement-focused approach, stating in its Regulatory Action Policy that it will assess whether a fine is required on the basis of the impact of any breach and the relevant organisations' culpability. While we await the upcoming UK statutory guidelines on enforcement action, it is noteworthy that the ICO has issued fines in two cases under the UK GDPR so far in 2021, against charities Mermaids and HIV Scotland, for failing to keep users' data (including 'special-category' data) secure. This suggests that the ICO's focus is shifting from large-scale breaches to the processing of 'higher risk' data; notably, neither of the 2021 cases involved a cyber-attack.

This is consistent with the ICO's statement on its priorities in July 2021, which emphasised that fines and penalties are "always a last resort" (as evidenced by the ICO's October 2020 enforcement notice ordering Experian to take specified corrective measures within nine months or face a fine). The ICO also stated that "helping [organisations] make changes and improvements to comply with the law", is the most effective way of reducing data malpractice. For example, well ahead of the EDPB draft guidelines, the ICO introduced its own guidance (including an interactive tool) to help organisations assess data breach notifications, which could be a possible factor in the reduction in notifications in the UK.[2] The ICO has otherwise reiterated its commitment to tackling nuisance marketing under the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("**PECR**"), having issued 63 penalties under PECR since May 2018 against just six under the nascent GDPR regime.

In September 2021, the UK Government's Department for Digital, Culture, Media and Sport (the "**DCMS**") proposed reforms to the UK's data protection regime in 'Data: a New Direction'. Proposals included refocusing the ICO on "the most serious threats and barriers to public trust and responsible data use" (rather than high-volume, low-level complaints). The DCMS recommended that only data breaches posing a material risk to a data subject should be notified (a proposal cautiously welcomed by the ICO), which could accelerate the downward trend in breach notifications.[3] Significantly, the DCMS proposed that PECR breaches should be subject to the maximum GDPR fines. The proposals suggest a refocusing on the greatest risks of harm to data rights - a view reportedly shared by new Information Commissioner, John Edwards.

Convergence on the risk of harm

Meanwhile, it is possible to see some broader convergence across the EU and UK towards prioritising enforcement in cases involving a more significant risk of harm to data rights and freedoms, albeit by different procedural routes.

EU DPAs have focused their enforcement activity on high-risk sectors (particularly big tech and telecoms) and regard compliance with the general GDPR principles as the best means of safeguarding data rights and freedoms. Enforcement actions by EU DPAs show that failing to comply with these principles, whether by unlawful data processing or a lack of transparency as to the basis or extent of processing, will lead to major fines (evidenced in the Amazon and WhatsApp decisions).

That is not to say that UK data breach cases will not lead to enforcement. Rather, the ICO seems to be increasingly attentive to the practical steps taken by data controllers in relation to risks faced. For example, post-breach investigations commonly require controllers to demonstrate that they know what data they have (as controller or processor), the nature of that data (for the assessment of the implications of any confidentiality or security breach) and the actions to minimise the risk to that data (including the implementation of sufficient IT security).[4] In circumstances where ransomware and other cyber-attacks are all too common, the ICO helpfully appears to recognise that 'appropriate technical and organisational measures' cannot mean 'perfect' measures, and controllers should not be held to an impossibly high standard (especially in cases where harm or the risk of harm is minimal).

Challenges to GDPR enforcement

Whether converging or diverging on the substance, common challenges to the enforcement process include limited resources, timing constraints and uncertainty.

[1] https://ico.org.uk/media/about-the-ico/consultations/2618333/ico-draft-statutory-guidance.pdf

[2] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/07/ico-s-priorities-and-impact-of-our-work/

[3] https://www.gov.uk/government/consultations/data-a-new-direction

[4] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/07/ico-s-priorities-and-impact-of-our-work/

Practical barriers

One of the most prevalent criticisms is that DPAs are too slow to take action on GDPR breaches.

The 'one-stop shop' mechanism is cited as a key reason for delays, placing responsibility for investigating the most prominent tech companies on just two DPAs (as the majority of such companies have their European headquarters in Luxembourg or Ireland). The CNPD and DPC have been characterised as more pro-business (and potentially 'softer' on controllers). The CNPD took until June 2021 to publish its first GDPR enforcement decision. The Irish Council for Civil Liberties reported that the DPC has failed to send draft decisions to its European counterparts in 98% of the major EU-wide cases for which it is responsible.[5]

Limited DPA resourcing can also impact on the ability to scrutinise controllers and handle complaints promptly. The EDPB reported in August 2021 that 86% of DPAs consider that they do not have adequate human resources to effectively carry out their activities.

The UK has invested considerably in the ICO (now the single largest DPA in Europe), but has just 13 people on its cyber-investigations team (1.7% of its full-time staff). The ICO was forced to suspend its investigation into real-time bidding and the Adtech industry between May 2020 and January 2021 due to pressure on resources during the COVID-19 pandemic.[6] Many controllers reporting cyber incidents in 2020/2021 have experienced delays in the ICO progressing (or closing) their cases.

Practical steps controllers can take to assist investigations include: (i) responding to the ICO's questions fully and promptly; (ii) maintaining close contact with the ICO via a DPO or otherwise; and (iii) investigating the incident themselves and proactively presenting clear facts from the outset.

A desire for direct redress, shifts in the claim-funding market and perceived delays in regulatory action have driven an increase in civil actions brought by individuals and NGOs seeking redress for breaches of data rights (including through collective actions). For instance, the ICO has been investigating TikTok's processing of children's data since March 2019, but former Children's Commissioner Anne Longfield launched a group action in April 2021 to obtain compensation for users (and so encourage substantive change by TikTok). Similarly, in April 2021, as the DPC announced its investigation, Digital Rights Ireland launched a group action to recover compensation for a 2021 Facebook data breach.

Appeals and uncertainty

However, DPAs are vulnerable to challenge and a number of enforcement fines have been successfully overturned or reduced on appeal. This may well lead to a reluctance on the part of DPAs to reach definitive conclusions quickly or without exhaustive evidence.

The ICO's £275,000 fine imposed on Doorstep Dispensaree Ltd ("**Doorstep**") in 2019 was reduced to £92,000 on appeal to the First-Tier Tribunal ("**FTT**") in August 2021. Doorstep's own investigation demonstrated that much of the evidence relied on by the ICO to set the fine had been gathered by another regulator for a different purpose and was inaccurate regarding the number of documents and data contained therein. This demonstrates the importance of data controllers carrying out their own investigation to establish the facts underpinning alleged GDPR breaches, and the appetite of the FTT to hold the ICO to account.

Ticketmaster's appeal of its £1,250,000 penalty notice to the FTT has been stayed pending the outcome of a parallel High Court collective action (which would materially assist the Tribunal on related issues of fact and law). The stay reveals the challenge posed by litigation to 'closing' regulatory issues. However, the recent UK Supreme Court decision in Lloyd v Google has closed the door for now on data-related opt-out representative claims for damages absent proof of actual harm. It therefore remains to be seen whether it will now be attractive for litigation funders to fund cases that may only lead to an award of damages once proven at a second stage, and whether the trend of significant litigation overshadowing enforcement will be sustained.

Given the deterrent effect of the largest fines, DPAs will be closely watching Amazon's appeal before the Luxembourg Administrative Tribunal. Amazon contends that the CNPD's decision was predicated on "subjective and untested interpretations of European privacy law". Paul Nemitz, Principal Adviser on Justice Policy, EU Commission and one of the architects of the GDPR, has stated that its fining system is inspired by the methodology of fines in EU competition law[7] (a statement echoed by the EDPB in the WhatsApp decision at para. 411). Tech giants are likely to pursue arguments similar to those already tested in the competition litigation space, including challenging jurisdiction, remedy and proper process.

Similarly, WhatsApp is taking a multi-pronged approach to challenging its recent fine, initiating: (i) a statutory appeal in Ireland; (ii) judicial review proceedings before the Irish High Court; and (iii) an EU court appeal against the EDPB, arguing that it interferes with its constitutional rights and is incompatible with the ECHR. These arguments echo those heard historically in CJEU tax litigation that used EU

[5] https://www.iccl.ie/wp-content/uploads/2021/09/Europes-enforcement-paralysis-2021-ICCL-report-on-GDPR-enforcement.pdf

[6] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/05/ico-statement-on-adtech-work/

[7] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3270535

freedoms to limit the ability of member states to levy taxes. The decision to directly pursue the EDPB is unprecedented and could result in concurrent domestic and EU-level appeals against the same decision.

Even the 'tougher' DPAs struggle with this challenge, evidenced by the Bonn Regional Court's strong criticism of the fining guidelines applied by the German DPAs in its November 2020 decision on the appeal by 1&1 Telecom GmbH – which saw the fine reduced by 90% on appeal.

Data controllers under investigation (or those appealing a decision) should also take note of the August 2021 decision by the Norwegian Privacy Appeals Board to reduce a fine imposed by Datatilsynet, the Norwegian DPA, criticising its unreasonably lengthy case-processing time (of over two years).

Conclusion

Despite an apparent divergence in approaches to GDPR enforcement and fines across the EU and the UK over the past three years, DPAs appear to be prioritising enforcement in cases where there is a more significant risk of harm to the rights and freedoms of data subjects (albeit using different regulatory tools and with parallel guidance from the EDPB and ICO).

From a UK perspective, and encouragingly for business and innovation, the ICO appears to be embracing a risk-based approach with a higher reporting threshold and a greater focus on reserving the most serious sanctions for those who mishandle or misuse data. By avoiding wielding the UK GDPR as a blunt instrument, the ICO may reduce the pressure on its limited resources in the long term and bolster its public perception as a protector of data subjects whose rights are seriously threatened.

A valuable lesson for data controllers from the range of enforcement decisions across the EU and UK is the importance of being able to demonstrate that they have 'got the basics right'. Controllers must keep track of how they use data, who they share it with, and where it sits, and should prepare for proactive, effective and sustained engagement with DPAs when an incident has occurred.

Slaughter and May advises on all aspects of data privacy law, including regulatory considerations following data breaches, and has extensive experience acting on group litigation proceedings before the English courts.

CONTACT

RICHARD JEENS
PARTNER
T: 02070905281
E: Richard.jeens@slaughterandmay.com

WILLIAM DOYLE
ASSOCIATE
T: 02070904736
E: William.doyle@Slaughterandmay.com

ROSS O'MAHONY
ASSOCIATE
T: 002070903856
E: ross.o'mahony@slaughterandmay.com

ALEX BUCHANAN
TRAINEE SOLICITOR
T: 02070904045
E: alex.buchanan@Slaughterandmay.com